



Фишинг в электронных деньгах

Лиенко Светлана

руководитель отдела по работе с клиентами
аккредитованного регистратора
доменных имен REG.RU

Типичные нарушения при использовании доменных имен

☠ Тайпсквоттинг

☠ Дорвей

☠ Фишинг

☠ Киберсквоттинг



Российский регистратор доменных имен

reg.ru

Тайпсквоттинг

- ✓ Регистрация доменных имён, близких по написанию с адресами популярных сайтов, в расчёте на ошибку части пользователей.

Например:

«wwwsite.ru» в расчёте на пользователя, который хотел попасть на «www.site.ru».

Интересно:

Популярный сайт сервиса «Одноклассники» имеет более 60 вариантов написания

Дорвей

- ✓ Входная страница — вид поискового спама, веб-страница, специально оптимизированная под один или несколько поисковых запросов с единственной целью её попадания на высокие места в результатах поиска по этим запросам.



Российский регистратор доменных имен

reg.ru

ФИШИНГ

- ✓ Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей.

Интересно:

За последние 3-и года компания REG.RU прекратила работу более 30 доменных имен, маскирующихся под систему WebMoney или сервисы этой компании.



Российский регистратор доменных имен

reg.ru

Киберсквоттинг

- ✓ Приобретение доменных имён, созвучных названиям известных компаний, или просто с «дорогими» названиями, с целью их дальнейшей перепродажи или размещения рекламы.

Часто киберсквоттинг сопровождается шантажом и угрозами в адрес правообладателей или заинтересованных лиц.

Угрозы, связанные с DNS

Различные способы «навредить» сайту с помощью DNS / системы доменных имён:

 Прекращение работоспособности домена

 Размещение нежелательного контента

— Фишинг

— «Дефейс»

— Дезинформация о компании / чёрный PR

Механизмы борьбы с указанными угрозами

Домен .РФ

5.6. Регистратор обязан приостановить делегирование доменного имени со списком серверов DNS, указанных администратором, в случаях:

...

- на основании мотивированного решения (запроса) в письменной форме одного из руководителей (заместителей руководителя) органа, осуществляющего оперативно-розыскную деятельность, в случаях, установленных федеральными законами; блокировка осуществляется до ее отмены судом либо органом, вынесшим решение о приостановлении делегирования;

- предусмотренных пунктами 9.12 настоящих Правил или условиями договора об оказании услуг регистрации доменных имен.

9.12. Регистратор обязан приостановить делегирование доменного имени в случае неисполнения администратором запроса регистратора, касающегося сведений, необходимых для идентификации в сроки, установленные в пункте 9.10 настоящих Правил.

Механизмы борьбы с указанными угрозами

Домен .РФ

9.14. Регистратор вправе приостановить делегирование домена незамедлительно без направления запроса, если им получена информация о недостоверности содержащихся в реестре сведений, необходимых для идентификации администратора.

Инструменты анализа и выявления фактов нарушений в качестве превентивных средств

Поиск схожих по написанию доменов (тайпсквоттинг/фишинг)

Домен содержит: Точное соответствие

Зарегистрирован с по

Оплачен до с по

Администратор содержит: Точное соответствие

ПРИМЕНИТЬ ФИЛЬТР **УБРАТЬ ФИЛЬТР**

« « 1 2 3 4 5 6 7 8 9 10 ... » »

Позиций: 1630, страниц: 33 Данные действительны на 08.02.2011 23:59:59

| Имя домена ▲ | Зарегистрирован | Оплачен до | Администратор | Регистратор |
|--|-----------------|------------|---|-------------------------------------|
| 1 007ODNOKLASSNIKI.RU | 2011-01-13 | 2012-01-13 | Garant-Park-Telecom LTD | R01-REG-RIPN |
| 2 00DNOKLASSNIKI.RU | 2011-01-25 | 2012-01-25 | Private Person | RUCENTER-REG-RIPN |
| 3 152ODNOKLASSNIKI.RU | 2010-05-11 | 2011-05-11 | High Tech Investments LTD | RU-CENTER-REG-RIPN |
| 4 1GOLYE-ODNOKLACNIKI.RU | 2009-12-02 | 2010-12-02 | | |
| 5 1ODNOKLASSNIKI.RU | 2009-03-29 | 2010-03-29 | | |
| 6 2011-ODNOKLASSNIKI.RU | 2010-12-16 | 2011-12-16 | Private Person | REGRU-REG-RIPN |
| 7 24ODNOKLASSNIKI.RU | 2009-01-22 | 2012-01-22 | Private Person | CENTROHOST-REG-RIPN |
| 8 2ODNOKLASSNIKI.RU | 2009-09-30 | 2011-09-30 | Aleksej A Yacura | REGTIME-REG-RIPN |
| 9 3DODNOKLASSNIKI.RU | 2010-01-26 | 2011-01-26 | Philipp A Gross | REGRU-REG-RIPN |
| 10 4ODNOKLASS.RU | 2010-12-21 | 2011-12-21 | Garant-Park-Telecom LTD | R01-REG-RIPN |
| 11 69ODNOKLASSNIKI.RU | 2010-03-25 | 2011-03-25 | Private Person | RU-CENTER-REG-RIPN |
| 12 7ODNOKLASSNIKI.RU | 2008-07-26 | 2009-07-26 | | |
| 13 ABOUT-ODNOKLASSNIKI.RU | 2010-02-03 | 2012-02-03 | Private Person | REGRU-REG-RIPN |
| 14 ACTION-ODNOKLASSNIKI.RU | 2010-10-20 | 2011-10-20 | Private Person | REGRU-REG-RIPN |
| 15 ADD-ODNOKLASSNIKI.RU | 2010-11-12 | 2011-11-12 | Private Person | REGRU-REG-RIPN |

Инструменты анализа и выявления фактов нарушений в качестве превентивных средств

Поиск схожих по написанию доменов (тайпсквоттинг/фишинг)

Домен содержит: Точное соответствие

Зарегистрирован с по

Оплачен до с по

Администратор содержит: Точное соответствие

E-mail администратора:

Регистратор: Количество строк:

Позиций: 167, страниц: 4

Данные действительны на 08.02.2011 23:59:59

| Имя домена ▲ | Зарегистрирован | Оплачен до | Администратор | Регистратор |
|--|-----------------|------------|--|-----------------------------------|
| 1 24ОДНОКЛАСНИКИ.РФ | 2010-11-27 | 2011-11-27 | Private Person | CENTROHOST-REG-RF |
| 2 АВТО-ОДНОКЛАСНИКИ.РФ | 2010-11-12 | 2011-11-12 | Private Person | REGRU-REG-RF |
| 3 АВТООДНОКЛАСНИКИ.РФ | 2010-11-12 | 2011-11-12 | R01 Personal Data Operator protected | R01-REG-RF |
| 4 АКЦИЯ-ОДНОКЛАСНИКИ.РФ | 2010-11-27 | 2011-11-27 | Private Person | NAUNET-REG-RF |
| 5 В-ОДНОКЛАСНИКАХ.РФ | 2010-11-12 | 2011-11-12 | Private Person | REGRU-REG-RF |
| 6 В-ОДНОКЛАСНИКИ.РФ | 2010-11-16 | 2011-11-16 | Private Person | REGRU-REG-RF |
| 7 ВИН-ОДНОКЛАСНИКИ.РФ | 2010-12-01 | 2011-12-01 | Private Person | NAUNET-REG-RF |
| 8 ВИП-ОДНОКЛАСНИКИ.РФ | 2010-11-27 | 2011-11-27 | Private Person | NAUNET-REG-RF |
| 9 ВКОНТАКТЕ-ОДНОКЛАСНИКИ.РФ | 2010-11-12 | 2011-11-12 | Private Person | NAUNET-REG-RF |
| 10 ВКОНТАКТЕ-ОДНОКЛАСНИКИ.РФ | 2010-11-23 | 2011-11-23 | Private Person | REGGI-REG-RF |
| 11 ВКОНТАКТЕОДНОКЛАСНИКИ.РФ | 2010-11-23 | 2011-11-23 | Private Person | REGGI-REG-RF |
| 12 ВОДНОКЛАСНИКИ.РФ | 2010-11-28 | 2011-11-28 | Private Person | REGRU-REG-RF |
| 13 ВОДНОКЛАСНИКАХ.РФ | 2010-11-12 | 2011-11-12 | R01 Personal Data Operator protected | R01-REG-RF |
| 14 ВОДНОКЛАСНИКИ.РФ | 2010-11-28 | 2011-11-28 | Private Person | REGRU-REG-RF |

| Домен / Посещаемость | CY | PR | руб. |
|----------------------|----|----|----------|
| trendex.ru | 2 | 0 | 4 750.00 |
| maxcoma.ru | 1 | 0 | 2 225.00 |
| mskdip.ru | 0 | 0 | 2 225.00 |
| geniusweb.ru | 1 | 0 | 2 225.00 |



Российский регистратор доменных имен

reg.ru

Инструменты анализа и выявления фактов нарушений в качестве превентивных средств

История данных Whois по домену

История Whois по доменам зоны .RU

Введите имя домена полностью:

ПОИСК

Пример: *reg.ru*

с 26.07.2007 по 06.10.2007:

domain: ODNOKLASSNIKI.RU
type: CORPORATE
nserver: ns3.nic.ru
nserver: ns4.nic.ru
nserver: ns8.nic.ru
state: REGISTERED, DELEGATED
org: [LTD "Odnoklassniki"](#)
phone: +7 926 4467195
e-mail: [company\[at\]odnoklassniki\[dot\]ru](mailto:company[at]odnoklassniki[dot]ru)
registrar: [RUCENTER-REG-RIPN](#)
created: 2002.01.15
paid-till: 2008.01.15
source: TC-RIPN

с 07.10.2007 по 12.10.2007:

domain: ODNOKLASSNIKI.RU
type: CORPORATE
nserver: ns3.nic.ru
nserver: ns4.nic.ru
nserver: ns8.nic.ru
state: REGISTERED, DELEGATED
org: [LTD "Odnoklassniki"](#)
phone: +7 925 5458055
e-mail: [company\[at\]odnoklassniki\[dot\]ru](mailto:company[at]odnoklassniki[dot]ru)
registrar: [RUCENTER-REG-RIPN](#)
created: 2002.01.15
paid-till: 2008.01.15
source: TC-RIPN

с 13.10.2007 по 31.10.2007:

domain: ODNOKLASSNIKI.RU
type: CORPORATE
nserver: ns3.nic.ru
nserver: ns4.nic.ru
nserver: ns8.nic.ru
state: REGISTERED, DELEGATED
org: [LTD "Odnoklassniki"](#)
phone: +7 495 662 6717
e-mail: [company\[at\]odnoklassniki\[dot\]ru](mailto:company[at]odnoklassniki[dot]ru)
registrar: [RUCENTER-REG-RIPN](#)
created: 2002.01.15



Российский регистратор доменных имен

reg.ru

Инструменты анализа и выявления фактов нарушений в качестве превентивных средств

Как правильно
считывать данные Whois

Информация о доменах (Whois) / IP / DNS

Тип запроса: информация о домене

Домен: **odnoklassniki.ru**

Статус: **зарегистрирован, [подобрать похожий свободный домен](#)**

IP-адрес: 217.20.144.194

По данным whois.ripn.net:

```
domain:      ODNOKLASSNIKI.RU
nserver:    ns.odnoklassniki.ru. 217.20.146.250
nserver:    ns.videogaga.ru.
nserver:    ns1.odnoklassniki.ru. 217.20.145.126
state:      REGISTERED, DELEGATED, VERIFIED ←
org:        LTD "Odnoklassniki"
phone:      +7 495 649 3099 ←
e-mail:     company@odnoklassniki.ru ←
e-mail:     site.management@odnoklassniki.ru ←
registrar:  RUCENTER-REG-RIPN ←
created:    2002.01.15
paid-till:  2012.01.15 ←
source:     TCI
```

[ПОСМОТРЕТЬ ИСТОРИЮ ДОМЕНА НА САЙТЕ STAT.REG.RU](#) >



Фишинг в электронных деньгах

Вопросы